Presidenza della Giunta

Ufficio Società dell'Informazione

ALLEGATO C

Procedura Aperta per la realizzazione dei servizi di rilascio e gestione della Firma Digitale ai cittadini della Basilicata

CAPITOLATO TECNICO

SOMMARIO

1. Introduzione al documento 4
1.1. Scopo e campo di applicazione del documento 4
1.2. Riferimenti normativi 6
2. Contesto di riferimento 7
2.1 Regione Basilicata 7
2.2. Durata e volumi della fornitura 10
3. Oggetto della fornitura 10
3.1. Specifiche tecniche 11
3.1.1. Il CMS 11
3.1.2. Dispositivi compresi nella fornitura 13
3.1.3. Materiale complementare 16
3.1.4. Certificati 18
3.1.5. Gestione e durata dei certificati 20
4. Connessione 21
5. Formazione 21
6. Supporto e assistenza 22
7. Manutenzione 23
8. Sito Web 23
9. Prestazioni e SLA 24
9.1. Disponibilità della soluzione 24
9.2. Disponibilità sospensione, riattivazione, revoca 24
9.3. Disponibilità sito web 24
9.4. Disponibilità assistenza 24

9.5. Disponibilità dell'interrogazione sullo stato dei certificati e tempestività di pubblicazione del loro stato 24

10. Promozione e comunicazione 24

11. Dismissione della fornitura 25

1. Introduzione al documento

1.1. Scopo e campo di applicazione del documento

PREMESSA

La Regione Basilicata promuove la diffusione delle tecnologie digitali per favorire l'accesso ai servizi pubblici, la trasparenza, la semplificazione dei processi, la cooperazione tra le pubbliche amministrazioni.

Il presente documento descrive il progetto di diffusione della Firma Digitale ai cittadini della Basilicata al fine di garantire l'utilizzo dei servizi di Identità Digitale della Pubblica Amministrazione e abilitare l'utenza all'accesso ai servizi on-line della rete telematica regionale.

Si vuole intercettare, inizialmente, la fascia di cittadini che è già utente di servizi avanzati su internet, quali, ad esempio, la Posta Elettronica Certificata, i procedimenti amministrativi, i servizi del portale Basilicatanet.

Tale utenza avanzata è stimata, anche sulla base di esperienze analoghe di altre regioni italiane, in circa il 5% della popolazione. Si ritiene tuttavia che questa fascia di utenti leader possa contribuire, nel tempo, a fare da traino per fasce sempre più vaste di cittadini, man mano che si presenterà un progressivo incremento di servizi on-line della PA. In questo modo, si contribuirà in modo sostanziale all'abbattimento del *Divario Digitale* e alla rimozione degli ostacoli che di fatto impediscono la piena parità di accesso alle informazioni e alle tecnologie dell'informazione e della comunicazione, tenendo conto in particolare delle situazioni di disabilità, disagio economico e sociale e diversità culturale.

LA FIRMA DIGITALE

La Firma digitale è particolare certificato elettronico che può essere memorizzato su un dispositivo hardware come una smart card o una penna USB dotata di microprocessore e che ha la finalità di agevolare il rapporto tra Cittadini, Imprese e Pubblica Amministrazione. Attraverso l'uso di questa

smart card intelligente è possibile accedere ai servizi on line erogati dalla Pubblica Amministrazione garantendo il riconoscimento dell'identità digitale del Cittadino e tutelandone, al contempo, la privacy.

La Regione Basilicata rilascerà la Firma Digitale su Pen Drive (chiavetta USB che non richiede l'uso di un lettore di smart card). E' previsto anche il rilascio della Firma Digitale da remoto nei casi in cui gli utenti non potranno disporre del dispositivo di Firma Digitale.

Il dispositivo servirà per:

- Firmare digitalmente un documento informatico per garantirne la validità a norma di legge;
- Autenticarsi ai servizi on-line della rete telematica regionale e di altre Pubbliche Amministrazioni;
- Eseguire i pagamenti on-line mediante transazioni telematiche protette;

Il Dispositivo di Firma Digitale (DFD) sarà consegnato gratuitamente a tutti i cittadini della Regione Basilicata che lo richiederanno.

Nel **microprocessore** saranno riportati i dati personali del titolare (nome, cognome, data e luogo di nascita, residenza e domicilio, codice fiscale). Nel microprocessore saranno inoltre registrati e rilasciati, da parte di specifiche Autorità di Certificazione nazionale, i certificati di identità e firma digitale che consentiranno di individuare in modo univoco l'identità del cittadino.

Per la diffusione del servizio e per agevolare l'accesso ai servizi on line da parte dei cittadini, verrà istituito un servizio regionale di Certificazione e Rilascio della Firma Digitale che prevede l'attivazione di strutture territoriali periferiche denominate **Sportelli al Cittadino**.

PIANO D'AZIONE PER LA DIFFUSIONE DELLA FIRMA DIGITALE

Verrà istituita una "Certification Autority per l'emissione e la consegna della Firma Digitale". Saranno intraprese le seguenti azioni:

1. Gara per l'individuazione di un soggetto a cui affidare l'attivazione dei servizi di rilascio e gestione delle Firme Digitali. I servizi oggetto del presente capitolato sono di seguito

riportati. Il costo complessivo dell'intervento è pari a **€. 1.000.000,00** IVA esclusa, per la durata triennale dell'appalto, e si riferisce a:

- Fornitura dei dispositivi di Firma Digitale e Firma Digitale da remoto (in questo secondo caso il servizio è rivolto ai soli dipendenti pubblici locali);
- Fornitura di un Card Management System per l'attivazione della firma digitale e per la gestione del ciclo di vita dei certificati (attivazione, revoche e sospensioni dei certificati);
- Fornitura del sito web tematico della firma digitale;
- Fornitura del servizio di registrazione e rilascio della Firma Digitale al cittadino e descrizione del relativo modello organizzativo;
- Formazione ed assistenza all'uso dei sistemi oggetto della fornitura, anche attraverso strumenti di *e*Learning;
- Fornitura dei servizi di assistenza tecnica e sistemistica;
- Attivazione dell'infrastruttura HW e dei sistemi di Disaster Recovery, Business Continuity, BackUp;
- Servizi di marketing e comunicazione per promuovere l'uso della Firma Digitale e l'accesso ai servizi della rete.

Non sono oggetto della presente gara i servizi di Call Center di I livello ed i servizi di back office di II livello, che saranno oggetto di successivi interventi e/o si avvarranno di servizi già attivi presso la Regione Basilicata.

Il costo per l'espletamento dei servizi del triennio successivo al primo, subordinato all'esercizio dell'opzione mediante procedura negoziata ai sensi dell'art. 57, c. 5, lett. b) del D. Lgs 163/06, di € 1.000.000,00, è da considerarsi quale stima di importo massimo e si riferisce al mantenimento, gestione ed assistenza dei servizi sopra elencati ed alla fornitura di ulteriori dispositivi di firma digitale in relazione alla valutazione da parte degli uffici regionali competenti, fatta sulla base dell'andamento delle richieste da parte dei cittadini.

1.2. Riferimenti normativi

- Decreto Legislativo 7 marzo 2005, n. 82, e successive modificazioni, recante il Codice

dell'Amministrazione Digitale e, in particolare, il capo II, che disciplina le firme elettroniche ed i certificatori, e l'art. 71, comma 1;

- Decreto Legislativo 30 giugno 2003, n. 196, e successive modificazioni, recante codice in materia di protezione dei dati personali;
- Decreto del Presidente del Consiglio dei Ministri 30 marzo 2009, recante le regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici, pubblicato nella Gazzetta Ufficiale 6 giugno 2009, n. 129;
- Direttiva 1999/93/CE del Parlamento Europeo e del Consiglio del 13 dicembre 1999, relativa ad un quadro comunitario per le firme elettroniche;

2. Contesto di riferimento

2.1 Regione Basilicata

INFRASTRUTTURE E SERVIZI DELLA RETE TELEMATICA

Il tema della Società dell'Informazione, come anche quello della Ricerca ed Innovazione, a livello di programmazione della Regione Basilicata, rientra in quello più generale della Società della Conoscenza, il cui obiettivo è quello di promuovere lo sviluppo di una società fondata sull'economia della conoscenza, attraverso il potenziamento della ricerca, la diffusione delle innovazioni e lo sviluppo delle reti ICT.

L'obiettivo specifico del piano strategico per lo sviluppo della Società dell'Informazione è articolato in due obiettivi operativi:

- Potenziamento delle reti regionali dell'ICT.
- Rafforzamento dei processi di innovazione della PA mediante il ricorso alle nuove Tecnologie dell'Informazione e Comunicazione;

In tale contesto, l'Ufficio Società dell'Informazione è l'attore principale nella definizione delle

politiche di innovazione per l'*e*Government e la Società dell'Informazione a livello regionale. Ha il compito di progettare e gestire gli interventi finalizzati a dotare il territorio regionale di un'infrastruttura a banda larga per collegare in rete gli enti centrali e periferici della Regione Basilicata, consentendo così la fruizione di servizi evoluti a cittadini e imprese. Di seguito vengono illustrati i programmi operativi, le linee di intervento ed i progetti di competenza dell'ufficio:

RETI E INFRASTRUTTURE

II.2.1.A: Completamento della copertura regionale della 'larga banda' nei territori in cui si registrano 'fallimenti di mercato' attraverso la realizzazione di impianti ed infrastrutture nonché acquisizioni di attrezzature in grado di assicurare standard di accesso e fruibilità tendenzialmente uniformi nell'intera regione.

II.2.1.B: Miglioramento degli standard di accessibilità e sicurezza, funzionalità ed operatività alla rete mediante l'adozione di tecnologie dell'informazione e della comunicazione mirati a garantire, agli utenti residenti, i diritti propri della 'cittadinanza elettronica'.

SERVIZI

II.2.2.A: Completamento e potenziamento della RUPAR, in modo da accrescere l'interoperabilità e la cooperazione nel settore pubblico regionale, anche attraverso l'attivazione di sistemi 'open source'.

II 2.2.B: Diffusione del sistema di e-government regionale con particolare riguardo agli enti locali minori a rischio di isolamento. Interventi previsti:

II 2.2.C: Implementazione di programmi comunitari come e-inclusion e e-health volti a ridurre gli svantaggi per individui e comunità (sviluppando, es., telemedicina e tele assistenza) ed a promuovere la partecipazione attiva dei cittadini (attivando, es., gli strumenti di e-democracy). Interventi previsti:

Le principali infrastrutture e servizi realizzati sono:

- **Infrastruttura di connettività e comunicazione** - Un'infrastruttura di comunicazione che colleghi tutte le Amministrazioni e riduca il Divario Digitale verso il cittadino.
- **Interoperabilità e cooperazione** – L'erogazione di servizi di intranet per la Pubblica Amministrazione (navigazione, posta elettronica, registrazione nomi a dominio, hosting web, servizi di registro, catalogo del riuso dei servizi); la definizione di regole e standard di interfaccia tra le Amministrazioni (Accordi di Servizio) per consentire comunicazioni efficienti e maggiore trasparenza verso l'esterno e, soprattutto, per ridurre il numero di interazioni del cittadino verso la Pubblica Amministrazione.
- **Autorità di Certificazione Locale** - La Regione Basilicata è Autorità di Certificazione Locale ed è struttura delegata al rilascio di strumenti per il riconoscimento dell'utente e della sua firma digitale (Carta Multiservizi) ed al rilascio di strumenti per la certificazione delle comunicazioni verso la Pubblica Amministrazione da parte dei Cittadini e delle Imprese (Posta Elettronica Certificata);
- **Bas-Anag – Circolarità Anagrafica Regionale** – il progetto prevede il raggiungimento dei seguenti due obiettivi: il potenziamento delle infrastrutture tecnologiche delle amministrazioni comunali per il collegamento con l'INA – Indice Nazionale delle Anagrafi – del Ministero dell'Interno; l'accesso, in cooperazione applicativa, da parte della Regione Basilicata ai dati certificati dal Ministero dell'Interno e pubblicati sul sistema INA/SAIA (ai fini di un loro utilizzo nei vari domini di interesse quali ad esempio Sanità, Lavoro, Semplificazione Amministrativa, etc.);
- **Portale Istituzionale** – Il Portale istituzionale della Regione Basilicata è raggiungibile all'indirizzo www.regione.basilicata.it. Attraverso il portale è possibile accedere ai servizi on-line dell'Ente e, quando previsto, accedere ai servizi in rete delle Pubbliche Amministrazioni;
- **Centro Servizi regionale** – I Centro Servizi eroga servizi di Call Center e di supporto alle strutture regionali e territoriali al fine di dare risposta ai cittadini su argomenti quali, ad esempio, prenotazioni prestazioni sanitarie, bandi, avvisi, assistenza, semplificazione amministrativa, eventi, etc;

2.2. Durata e volumi della fornitura

Il termine di esecuzione del progetto è di 36 mesi. Il servizio può essere rinnovato per ulteriori 36 mesi subordinatamente all'esercizio dell'opzione mediante procedura negoziata ai sensi dell'art. 57, c. 5, lett. b) del D. Lgs 163/06.

I volumi della fornitura riferiti al primo triennio non devono essere inferiori a 25.000 dispositivi di Firma Digitale come descritti nel successivo paragrafo. Sono inoltre richiesti almeno 1.500 Firme Digitali da Remoto per i dipendenti pubblici locali. Sono ammesse e saranno oggetto di valutazione premiante le offerte in aumento rispetto ai valori minimi stimati.

3. Oggetto della fornitura

La fornitura oggetto d'appalto comprende tutto quanto necessario a rendere la Stazione Appaltante in grado di emettere autonomamente, tramite postazioni di lavoro appositamente allestite, dispositivi Token USB recanti a bordo certificati di Firma Digitale e CNS. Sono considerati parte della fornitura anche i software e quanto necessario per l'utilizzo dei certificati emessi, i dispositivi da personalizzare, utilizzo e gestione degli stessi, tutto il materiale (sia digitale che non) di supporto ad un corretto e completo utilizzo dei prodotti e servizi oggetto della fornitura sia da parte della Regione Basilicata che di tutti gli utilizzatori finali dei dispositivi rilasciati.

In particolare, sono compresi nella fornitura:

- Il software di emissione dei certificati, Card Management System (CMS);
- L'infrastruttura hardware necessaria per consentire l'operatività e la raggiungibilità del software CMS e la fornitura del servizio in modalità ASP per tutta la durata del contratto;
- L'utilizzo di strumenti necessari alla verifica e alla gestione dei certificati emessi (ad es. CRL / OCSP);
- La licenza d'uso del software di firma da usare in abbinamento ai certificati e dispositivi rilasciati;
- La manutenzione e il supporto relativi a tutti i software oggetto di fornitura;

- I dispositivi Token USB e i chip crittografici sui quali verranno emessi i certificati;
- I manuali e la documentazione d'accompagnamento ai dispositivi;
- Il sito web di supporto al servizio;
- La formazione del personale individuato dalla Stazione Appaltante per l'erogazione del servizio all'utente finale; la formazione per i responsabili di dette figure;
- La fornitura dei servizi di marketing e comunicazione per promuovere l'uso della Firma Digitale e l'accesso ai servizi della rete.

Resta inteso che il fornitore si impegna all'allestimento di un sistema di emissione che possa essere raggiunto contemporaneamente da più postazioni client senza limitazioni operative ed utilizzato da comuni personal computer dotati di connessione ad internet/intranet; tipicamente:

- Personal computer con sistema operativo Windows XP o successivi;
- Browser Internet Explorer;
- Connessione internet etc;
- Conessione intranet etc;
- Altre specifiche (domini, policy di accesso ed utilizzo etc);

3.1. Specifiche tecniche

3.1.1. Il CMS

Caratteristiche del servizio offerto

Il sistema offerto dovrà essere ospitato, in modalità ASP, su architettura fisica e virtuale completamente ridondata in tutte le sue componenti. La soluzione sarà dunque completamente in outsourcing: il centro servizi, deputato alla gestione tecnica del CMS, dovrà essere ospitato presso un data center esterno per tutta la durata del contratto e non presso la server farm Regionale.

In sede di offerta tecnica il fornitore dovrà illustrare tutte le misure volte a garantire sicurezza, continuità, disponibilità del sistema che intenderà adottare.

Il fornitore dovrà farsi carico dell'installazione e configurazione e manutenzione delle macchine necessarie all'erogazione del servizio CMS e degli eventuali portali di progetto. Resta inteso che la Regione non si farà carico dell'acquisto delle macchine e degli apparati utilizzati per il funzionamento del CMS.

Il data center dovrà rispettare elevati standard di sicurezza e disporre di un presidio tecnico 24h su 24, 7 giorni su 7.

Gestione del ciclo di vita delle carte

Il fornitore dovrà mettere a disposizione un software CMS (Card Management System) che permetterà di gestire l'intero ciclo di vita delle carte.

Tale software dovrà gestire l'emissione delle carte CMS in modalità singola o bulk (emissione massiva centralizzata).

Dovrà poter essere possibile l'importazione, la gestione e l'attivazione di CNS emesse da enti diversi (quali ad esempio SOGEI).

Una carta CNS si considera attiva una volta assegnati i codici PIN e PUK, che ne permettono l'utilizzo al cittadino. Il CMS dovrà poter gestire l'attivazione delle carte CNS presso qualsiasi sportello regionale abilitato a prescindere dal luogo di residenza. Il fornitore dovrà pertanto individuare la soluzione che ritiene più opportuna per permettere la distribuzione sicura dei codici PIN e PUK.

Il fornitore dovrà prevedere tutti i processi che permettono la gestione completa del ciclo di vita delle carte, compresi blocco, sospensione, revoca e altre casistiche che possano verificarsi durante l'utilizzo della carta. Il CMS dovrà permettere la gestione dei processi così come delineati dal fornitore.

Il fornitore dovrà elencare le carte che il CMS è in grado di supportare.

Il CMS dovrà tracciare tutte le operazioni eseguite sullo stato delle carte. Inoltre dovrà prevedere la generazione di tutta una serie di report atti a fornire una documentazione analitica su tutte le attività di rilievo.
Il CMS dovrà essere un software modulare, multi-utente e dovrà gestire almeno i seguenti utenti:

- utente amministratore;
- utenti area amministrazione ente;
- utenti area ente sportelli;
- utente cittadino da Portale WEB;
- utente operatore Contact Center.

Dovrà esser sviluppato in architettura Java Enterprise Edition (J2EE). Dovrà inoltre essere garantita la sicurezza e la separazione dei dati: il fornitore dovrà descrivere le caratteristiche e funzionalità del CMS che permettono di fornire tale garanzia. Il fornitore dovrà garantire l'aggiornamento tecnico e normativo e la manutenzione evolutiva, descrivendo le modalità in cui intende adempiervi. Il CMS dovrà prevedere la possibilità di eventuale integrazione con altri sistemi della Regione. Il fornitore dovrà garantire manutenzione correttiva e dovrà descrivere i canali, le procedure di escalation e le modalità di comunicazione e gestione delle segnalazioni.
Il software fornito dovrà consentire la creazione di nuovi circuiti di emissione per altre e differenti tipologie di carte/certificati (ad.es. carte dei servizi, carte operatori sanitari etc).

3.1.2. Dispositivi compresi nella fornitura

Il sistema di emissione oggetto della fornitura dovrà essere in grado di rilasciare certificati di autenticazione e sottoscrizione su chip crittografico alloggiato, in fase di emissione dei certificati, su supporto plastico, in modo tale da poter completare il processo di personalizzazione dei chip

tramite comune lettore Smartcard con connessione USB. Terminata la personalizzazione elettrica del chip dovrà essere possibile isolare lo stesso dal supporto plastico, in modo tale da poterlo inserire in un secondo momento all'interno dei dispositivi Token USB che l'aggiudicatario comprenderà nella fornitura in numero non inferiore a 25.000. Tale accorgimento dovrà permettere, al momento della scadenza dei certificati CNS e di firma, di dover sostituire solo la smartcard fustellata e non l'intero dispositivo Token.

I dispositivi dovranno consentire la ricezione a bordo dei certificati generati nonché la loro conservazione e il loro utilizzo (a titolo esemplificativo, non esaustivo: firma e autenticazione, e, interfacciandosi con la CA sospensione, riattivazione, revoca).

Il sistema dovrà permettere l'assegnazione in maniera segreta e sicura dei codici di gestione della carta (PIN, PUK ed altri, se previsti dal processo di emissione e gestione proposto dall'aggiudicatario).

La fornitura di tutti i dispositivi sarà a carico del fornitore e il numero di dispositivi compresi nell'offerta sarà oggetto di valutazione e comparazione tra i partecipanti alla gara.

Nei paragrafi seguenti, i requisiti tecnici minimi ai quali le offerte, pena esclusione dovranno attenersi.

3.1.2.1. CHIP

I dispositivi di tipo "Smartcard" offerti dovranno essere conformi, aderenti e certificati secondo la normativa vigente in merito. Dovranno inoltre rispettare o superare, per la parte inerente al chip crittografico alloggiato, le caratteristiche espresse nella tabella sottostante.

Memoria eeprom	66k
Vita utile (cicli lettura/scrittura) eeprom	500.000
Sistema Operativo	Conforme alle specifiche CNS
APDU	Conforme ISO 7816-1,2,3,4,8,9

Lunghezza PIN/PUK	8 cifre
Blocco dell'accesso	al terzo inserimento PIN errato
Blocco irrevocabile del dispositivo	Al terzo inserimento PUK errato
Supporto degli algoritmi crittografici	RSA, AES, DES, 3DES
Supporto degli algoritmi di hashing	SHA1 e SHA256 on-chip
Chiavi RSA (lunghezza)	2048 bit
Tempo massimo di firma (con chiavi 2048 bits)	1403,34 msec
Ritenzione dei dati	10 anni minimo

Il supporto plastico dovrà essere in PVC laminato con overlay di protezione sui due lati giungere alla stazione appaltante già personalizzato con grafica in quadricromia stampata in offset, sulla base delle grafiche stabilite dalla Regione Basilicata.

La carta proposta dovrà rispettare:

- la normativa relativa alla Carta Nazionale dei Servizi;
- la normativa sulla firma digitale qualificata.

3.1.2.2. Token USB

I token USB compresi nell'offerta dovranno essere predisposti all'alloggiamento di chip rimovibili, aventi requisiti pari a quelli descritti nella tabella del precedente paragrafo.

I token USB dovranno inoltre:

- Avere una memoria flash di almeno 2Gb;
- Essere compatibili con Windows, Linux e MAC, ovvero dovrà funzionare con tutti e 3 i sistemi operativi senza dover sostituire dispositivo;
- Contenere un software di firma preinstallato;

- Consentire lo switch a lettore CCID (anche previa installazione di apposito software);
- Il software dovrà prevedere l'aggiornamento automatico in caso di rilascio di nuove versioni;

La personalizzazione grafica dei dispositivi Token USB (guscio plastico esterno) sarà a carico del fornitore, dovrà essere eseguita in tampografia, sulla base delle grafiche (file) consegnate all'aggiudicatario da Regione Basilicata.

3.1.3. Materiale complementare

Il fornitore dovrà illustrare nell'offerta tecnica le modalità che intende utilizzare per l'assegnazione dei codici PIN/PUK ai certificati/dispositivi, nonché i supporti, da consegnare all'utente finale, deputati alla custodia di tali codici. Requisito essenziale è l'assegnazione sicura dei codici pin e puk ai dispositivi, i quali dovranno comunque essere già pronti all'uso (tramite i codici assegnati) senza ricorrere a procedure di "sblocco" e/o "attivazione" di qualsiasi natura.

Sarà altresì compito della ditta aggiudicatrice fornire tutto il materiale digitale e cartaceo di supporto all'utilizzo dei servizi e dispositivi forniti.

3.1.3.1. Software di firma

E' considerata parte della fornitura la licenza d'uso di software di firma per l'utilizzo dei certificati rilasciati su dispositivo. Sarà cura del fornitore consegnare alla stazione appaltante dispositivi Token USB già contenenti un software che consenta l'utilizzo dei certificati prodotti dal CMS offerto.

Tale software dovrà essere appositamente concepito per l'utilizzo in abbinamento a dispositivi Token USB e non dovrà prevedere fasi di installazione necessarie al suo utilizzo.

Il software presente all'interno del Token USB dovrà inoltre auto-aggiornarsi all'avvio, previa connessione ad internet della postazione in uso, tutte le volte che il fornitore rilascerà aggiornamenti per il software in oggetto su server appositamente adibito allo scopo.

Una volta inserito il chip personalizzato all'interno del dispositivo, il software di firma dovrà consentire di effettuare operazioni di:

- Firma di file in formato .p7m (cades) e aggiunta firma a firme pre-esistenti;
- Firma di file in formato .pdf (pades) e aggiunte firma a firme pre-esistenti;
- Firma multipla: dovrà essere possibile, selezionando una cartella, firmare con una sola operazione tutti i file in essa contenuti;
- Apposizione di firme a differenti livelli gerarchici;
- Firma grafica: per le firme .pdf dovrà essere possibile apportare modifiche grafiche al file da firmare, a scelta dell'utente;
- Verifica di file firmati;
- Verifica dei certificati a bordo e del loro stato;
- Importazione dei certificati su browser;
- Gestione codici carta (cambio PIN; sblocco PIN; sblocco PIN con PUK);
- Cifratura/decifratura di file;

Il software dovrà inoltre consentire un'autodiagnosi del dispositivo e del chip contenuto, in maniera tale da agevolare le operazioni di assistenza da remoto e/o risoluzione autonoma delle criticità da parte dell'utente finale;

- Supporto per l'apposizione di marche temporali in linea con le seguenti specifiche: **Rfc 5544** (TimeStampData), **CAdES-T**, **PAdES**, **TST** e **TSR** (Rfc 3161);
- Supporto per la verifica di validità dei certificati tramite CRL e OCSP
- Supporto per interfacciamento PROXY (http, https, ldap e socks);
- Supporto per **TokenD** per consentire l'utilizzo delle funzioni di crittografia del chip anche da parte di quelle applicazioni che fanno uso del portachiavi di Macosx;

Il fornitore dovrà garantire la compatibilità del software inserito nel Token USB con sistemi operativi Windows (da XP in poi), MAC e Linux.

3.1.4. Certificati

I certificati generati dal CMS proposto e scaricati su dispositivo dovranno essere di due tipi:

- **Certificato di autenticazione CNS**: utilizzato principalmente per accedere in maniera sicura ai siti web delle Pubbliche Amministrazioni, secondo quanto previsto dal CAD (Codice dell'Amministrazione Digitale).
- **Certificato qualificato** di sottoscrizione, opzionalmente con ruolo: utilizzato per la firma digitale di documenti di qualsiasi natura, salvo eventuali limitazioni d'uso inserite nel certificato stesso;

Il sistema proposto dovrà consentire l'emissione di uno o entrambi i certificati su singolo chip, all'interno di una unica sessione di lavoro.

Resta inteso che i certificati dovranno essere conformi alle normative rispettivamente applicabili.

I certificati forniti dovranno avere una validità di 6 anni.

3.1.4.1. Requisiti del certificato di firma digitale emesso

Il certificato qualificato di sottoscrizione dovrà avere un profilo conforme alla vigente normativa in materia di firma digitale e in particolare a:

- D.Lgs. 7 marzo 2005, n. 82: "Codice dell'Amministrazione Digitale" (in breve: CAD) e successivi aggiornamenti e integrazioni;
- Decreto del Presidente del Consiglio dei Ministri 30 Marzo 2009: "Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici";

- Deliberazione CNIPA n.45/2009: “Regole per il riconoscimento e la verifica del documento informatico”.

Oltre all’indirizzo della CRL, il certificato dovrà contenere, nell’estensione AuthorityInfoAccess, l’indirizzo del server di validazione on-line (con protocollo OCSP), gestito dal fornitore.
In questo tipo di certificato dovrà essere possibile inserire opzionalmente anche il Ruolo del Titolare, inteso come il Titolo e/o Abilitazione professionale in possesso del Titolare del certificato, ovvero l'eventuale potere di rappresentare enti di diritto privato o pubblico, ovvero l'Appartenenza a detti enti nonché l'Esercizio di funzioni pubbliche.

Il ruolo potrà essere inserito nell’attributo title del campo Subject certificato, con la codifica specificata nelle “*Linee Guida per la certificazione delle qualifiche e dei poteri di rappresentanza dei Titolari dei certificati elettronici*” .

3.1.4.2. Requisiti del certificato CNS emesso

Il certificato di autenticazione dovrà avere un profilo conforme alle specifiche CNIPA: “Profilo di certificato digitale per l’autenticazione mediante Carta Nazionale dei Servizi (CNS)”.

Il valori “CN” e “OU” del campo Issuer del certificato saranno concordati con la Regione Basilicata. Su richiesta della Regione inoltre nel campo Subject del certificato dovranno poter essere inseriti, in aggiunta ai dati obbligatori previsti dalle specifiche DIGITPA, anche il nome e cognome del Titolare rispettivamente negli attributi givenName e surname.

Al fine di consentire al titolare di usare il certificato di autenticazione anche per la protezione della posta elettronica (cifratura e/o firma elettronica), dovrà essere possibile inserire in maniera opzionale:

- l’indirizzo di posta elettronica del titolare nell’attributo emailAddress del Subject;
- l’indirizzo di posta elettronica del titolare nella estensione SubjectAltName;

- il valore id-kp-emailProtection nell'estensione ExtendedKeyUsage;
- il valore keyEncipherment nell'estensione KeyUsage.

Oltre all'indirizzo della CRL (accessibile con due diversi protocolli: HTTP ed LDAP), il certificato dovrà contenere, nell'estensione AuthorityInfoAccess, l'indirizzo del server di validazione on-line (con protocollo OCSP), gestito dal fornitore.

3.1.5. Gestione e durata dei certificati

I certificati offerti dovranno avere una durata di 6 anni.

Per tutto il ciclo di vita dei certificati dovrà essere possibile, attraverso l'utilizzo di funzionalità apposite interne al CMS, sospendere, riattivare e revocare i certificati.

Tali operazioni, una volta richieste attraverso il sistema, dovranno risultare efficaci sullo stato di validità dei certificati (alla verifica della CRL) entro e non oltre 60 minuti dalla richiesta.

3.1.5.1 Servizi di verifica della validità dei certificati (CRL, OCSP)

Il fornitore dovrà rendere disponibili servizi di verifica della validità dei certificati in due diverse modalità, raggiungibili tramite HTTP e/o LDAP:

- pubblicazione e costante aggiornamento della Certificate Revocation List (CRL);
- erogazione di un servizio di validazione on-line basato sul protocollo OCSP.

Entrambe le modalità dovranno essere disponibili tutti i giorni dell'anno, 24 ore al giorno. E' requisito indispensabile che i servizi risiedano su infrastrutture di proprietà della società aggiudicatrice, la quale dovrà illustrare come e attraverso quali strumenti intende garantire la sicurezza e la continuità del servizio.

Sarà considerato un valore aggiunto l'utilizzo di uno o più dei seguenti strumenti:

- uso di un software OCSP responder di alta qualità ed elevate prestazioni;
- uso di un HSM (dispositivo crittografico hardware) ad elevate prestazioni;
- infrastruttura tecnologica ridondata a diversi livelli (elaboratori, connettività);
- monitoraggio costante dei sistemi e alerting automatico in caso di anomalie.

4. Connessione

Le postazioni che Regione Basilicata predisporrà all'emissione di certificati saranno dotate di accesso ad intranet ed internet. Il sistema proposto dall'aggiudicatario dovrà essere raggiungibile attraverso entrambi i canali. Nel caso della intranet, il fornitore dovrà garantire una connessione dedicata (Virtual Private Network) all'infrastruttura ospitante il servizio della portata di almeno 50mbit da dedicare in maniera esclusiva a Regione Basilicata per la fruizione del servizio. Sarà compito del fornitore illustrare le caratteristiche della connessione offerta, dando particolare risalto alla sicurezza e continuità del servizio.

5. Formazione

La società aggiudicataria dovrà organizzare ed erogare giornate di formazione per il personale indicato dalla Regione Basilicata.

In particolare, i corsi dovranno rivolgersi al personale di sportello deputato all'utilizzo del sistema proposto per l'emissione di certificati.

I corsi, comprensivi di prove pratiche e simulazioni, dovranno tenersi presso i luoghi indicati ed appositamente allestiti dalla Regione Basilicata. Non dovranno avere una durata superiore alla mezza giornata (4 ore lavorative consecutive), dovranno essere corredati di materiale didattico cartaceo e/o digitale a supporto dell'apprendimento dei discenti. Il personale docente messo a disposizione dovrà avere un'esperienza comprovata nel campo dell'insegnamento/erogazione corsi, nonché una comprovabile esperienza tecnica e normativa dei temi affini al servizio oggetto di gara. La Regione Basilicata stima che ogni corso vedrà la presenza di 12 partecipanti circa.

I concorrenti dovranno specificare le modalità in cui intendono organizzare la formazione degli addetti e specificare il numero di corsi compreso nell'offerta. In aggiunta, sarà facoltà dei concorrenti proporre giornate di affiancamento al personale delle sedi da avviare al servizio.

Sarà considerata elemento migliorativo la proposta di ulteriori e differenti soluzioni formative: verrà dato rilievo alle offerte in grado di curare concretamente le necessità di aggiornamento che l'erogazione del servizio potrà generare, così come le necessità di formazione di personale che la Regione Basilicata destinerà all'erogazione del servizio in momenti successivi alla fase di start-up.

6. Supporto e assistenza

Il fornitore dovrà garantire il servizio di assistenza, relativo a richieste di contatto provenienti sia dagli utilizzatori del CMS che dai titolari dei certificati, rispettando ed eventualmente migliorando i seguenti orari:

dal lunedì al venerdì: dalle 8.30 alle 18.30

Il sabato: dalle 8.30 alle 12.30

Le richieste di assistenza perverranno al fornitore dall'help desk di secondo livello già operativo per conto della Regione Basilicata. Agli operatori in forza al secondo livello dovrà essere data la possibilità di contattare il terzo livello messo a disposizione dal fornitore tramite i seguenti strumenti:

- Casella Email dedicata;
- Ticket;
- Numero di telefono dedicato;

A seguito della segnalazione avvenuta con uno dei diversi canali si dovrà provvedere all'apertura di un ticket-assistenza. Tali ticket dovranno garantire la tracciabilità delle richieste di assistenza, riportando una serie di informazioni, tra le quali:

- orario di apertura ticket
- stato della richiesta (presa in carico, in fase di elaborazione, risoluzione)

Il fornitore dovrà garantire la presa in carico entro 4 ore delle segnalazioni, rispettando i seguenti tempi di risoluzione:

- problematicità non bloccanti: entro 10 giorni solari continuativi dalla segnalazione;
- problematicità bloccanti: entro 3 giorni solari consecutivi dalla segnalazione.

7. Manutenzione

Il fornitore dovrà garantire per tutta la durata del contratto la manutenzione evolutiva e adeguativa dei sistemi offerti.

8. Sito Web

Il fornitore dovrà progettare, sviluppare e rendere disponibile un sito web di supporto e promozione del servizio. Dovranno essere pubblicate su detto sito tutte le informazioni necessarie ad illustrare in maniera esaustiva il servizio proposto, nonché tutti i manuali d'uso dei dispositivi e software inclusi nella fornitura così come tutta la documentazione ritenuta necessaria dalla normativa di riferimento. Nello specifico, il fornitore dovrà inoltre offrire la funzionalità di "content management system", in maniera tale da mettere la Stazione Appaltante in grado di variare, rimuovere e/o aggiungere agevolmente i contenuti del sito web in maniera autonoma. La disponibilità del sito web dovrà essere h24/365gg.

Sarà facoltà dei partecipanti illustrare funzionalità aggiuntive da rendere disponibili sul sito web proposto il quale dovrà in ogni caso prevedere la possibilità (per l'utente finale) di sospendere e riattivare i certificati attraverso apposite sezioni del sito web.

Resta inteso che tutto quanto necessario alla messa in esercizio del sito web in oggetto, del suo utilizzo, della sua gestione e allocazione è da considerarsi a carico dell'aggiudicatario. L'aggiornamento dei contenuti sarà invece a carico del personale regionale.

9. Prestazioni e SLA

9.1. Disponibilità della soluzione

La soluzione proposta dovrà essere disponibile tutti i giorni dell'anno, esclusi i giorni festivi nazionali e le domeniche, durante seguente orario almeno:

- Dal lunedì al venerdì, dalle 08:00 alle 18:00;
- Il sabato, dalle 08:00 alle 14:00

9.2. Disponibilità sospensione, riattivazione, revoca

Il fornitore dovrà garantire che le funzionalità di sospensione, riattivazione e revoca siano disponibili in modalità h24/365gg (tutti i giorni dell'anno, 24 ore al giorno).

9.3. Disponibilità sito web

Il sito web proposto dovrà avere una disponibilità non inferiore a quella garantita per la soluzione di emissione.

9.4. Disponibilità assistenza

La disponibilità del servizio d'assistenza dovrà essere conforme a quanto specificato nel cap.7.

9.5. Disponibilità dell'interrogazione sullo stato dei certificati e tempestività di pubblicazione del loro stato

Il fornitore dovrà garantire che gli strumenti che consentono la verifica della validità dei certificati, sia via CRL che OCSP, siano disponibili h24 tutti i giorni dell'anno. La pubblicazione delle CRL relative ai certificati di sottoscrizione e autenticazione dovrà essere aggiornata ogni ora.

10. Promozione e comunicazione

L'impresa dovrà indicare le modalità operative con le quali intende effettuare la promozione e diffusione della Firma Digitale e dei servizi realizzati nell'ambito del presente progetto, sia attraverso Internet sia con strategie tradizionali, come ad esempio manifesti, spot pubblicitari,

campagne di marketing, etc. Resta inteso che tutti gli oneri derivanti dal piano di promozione e comunicazione proposto sono a carico dell'offerente.

11. Dismissione della fornitura

L'Aggiudicatario della gara d'appalto si impegna a mantenere attivi tutti i servizi e le funzioni di Certification Authority anche dopo la cessazione del contratto, fintanto che i certificati emessi durante la fornitura saranno in corso di validità.

Tali attività comprenderanno:

- manutenzione, aggiornamento ed eventuale adeguamento normativo dei software forniti;
- le funzioni di sospensione, riattivazione e revoca – da parte chi, vedremo;
- la tenuta in esercizio degli strumenti per la verifica della validità dei certificati emessi (CRL, OCSP);

Su richiesta della Regione Basilicata il fornitore dovrà altresì consegnare tutti i dati inerenti al servizio nel suo complesso, raccolti durante il periodo di effettiva erogazione.